Math 357
Galois theory example

April 18, 2024

In these notes we use galois theory to analyze algebraic objects—zeros, field extensions, and groups—arising from the polynomial $f = t^3 - 2 \in \mathbf{Q}[t]$. We start with a summary of the story. We invite the reader to fill in details and justify the assertions before proceeding to following sections, in which we explore the story and logic together.

1 Overview

Let

$$f = t^3 - 2 \in \mathbf{Q}[t]$$

A splitting field for f is $K = \mathbf{Q}(\alpha, \zeta_3)$, where α is a zero of f, and ζ_3 is a zero of $g = t^2 + t + 1 \in \mathbf{Q}[t]$. A basis for K as a $\mathbf{Q}$-vector space is

$$\mathcal{B} = (1, \alpha, \alpha^2, \zeta_3, \zeta_3\alpha, \zeta_3\alpha^2)$$

The field extension $K : \mathbf{Q}$ is galois, with galois group

$$\mathrm{Gal}(K : \mathbf{Q}) = \langle \sigma, \tau \mid \sigma^3, \tau^2, (\sigma\tau)^2 \rangle$$

where the automorphisms $\sigma, \tau : K \to K$ are defined by

$$\begin{aligned} \sigma : \alpha &\mapsto \zeta_3\alpha & \qquad \tau : \alpha &\mapsto \alpha \\ \zeta_3 &\mapsto \zeta_3 & \zeta_3 &\mapsto \zeta_3^2 = -(1 + \zeta_3) \end{aligned} \tag{1}$$

One can use the galois correspondence between subfields and subgroups to enumerate and match all of each. In particular, the subfield $\mathbf{Q}(\zeta_3\alpha)$ corresponds to the subgroup $\langle \sigma^2\tau \rangle$. That is,

$$\mathcal{F}(\langle \sigma^2\tau \rangle) = \mathbf{Q}(\zeta_3\alpha) \qquad\qquad \mathrm{Aut}(K : \mathbf{Q}(\zeta_3\alpha)) = \langle \sigma^2\tau \rangle$$

2 Subfield–subgroup correspondence

Claim: $\mathcal{F}(\langle \sigma^2\tau \rangle) = \mathbf{Q}(\zeta_3\alpha)$.

To prove this claim, we show set containment in both directions. Recall that $\langle \sigma^2\tau \rangle = \{\mathrm{id}_K, \sigma^2\tau\}$, and the identity map id_K fixes all of K, and hence, in particular, $\mathbf{Q} \subseteq K$. Thus for the fixed-field computations here, it suffices to analyze $\sigma^2\tau$. (More generally, we need to analyze a set of generators of the subgroup.) Also recall that, by definition, ζ_3 is a zero of $g = t^2 + t + 1$, hence also a zero of $(t-1)g = t^3 - 1$. Explicitly writing out what these zeros mean, we get

$$\zeta_3^2 = -(1+\zeta_3) \qquad\qquad \zeta_3^3 = 1$$

($\supseteq$) Because $\sigma, \tau \in \mathrm{Gal}(K : \mathbf{Q}) = \mathrm{Aut}(K : \mathbf{Q})$, they are field homomorphisms. Using this fact and the defining images of σ and τ specified in equation (1), we compute

$$\begin{aligned}
\sigma^2\tau(\zeta_3\alpha) &= \sigma(\sigma(\tau(\zeta_3\alpha))) \\
&= \sigma(\sigma(\tau(\zeta_3)\tau(\alpha))) \\
&= \sigma(\sigma(\zeta_3^2 \cdot \alpha)) \\
&= \sigma(\sigma(\zeta_3)^2\sigma(\alpha)) \\
&= \sigma(\zeta_3^2 \cdot \zeta_3\alpha) = \sigma(\zeta_3^3\alpha) = \sigma(\alpha) \\
&= \zeta_3\alpha
\end{aligned}$$

Alternatively, we can use the same hypotheses to compute where $\sigma^2\tau$ sends each generator of $K = \mathbf{Q}(\alpha, \zeta_3)$:

$$\sigma^2\tau(\alpha) = \zeta_3^2\alpha \qquad\qquad \sigma^2\tau(\zeta_3) = \zeta_3^2 \tag{2}$$

to conclude that

$$\sigma^2\tau(\zeta_3\alpha) = \sigma^2\tau(\zeta_3) \cdot \sigma^2\tau(\alpha) = \zeta_3^2 \cdot \zeta_3^2\alpha = \zeta_3^4\alpha = \zeta_3\alpha$$

This shows that $\sigma^2\tau$ fixes the element $\zeta_3\alpha \in K$. Because $\sigma^2\tau \in \mathrm{Gal}(K : \mathbf{Q})$, $\sigma^2\tau$ also fixes the base field $\mathbf{Q}$. Hence $\sigma^2\tau$ fixes $\mathbf{Q}(\zeta_3\alpha)$. That is,

$$\mathbf{Q}(\zeta_3\alpha) \subseteq \mathcal{F}(\langle\sigma^2\tau\rangle) \tag{3}$$

($\subseteq$) To show the reverse inclusion, let $\beta \in \mathcal{F}(\langle\sigma^2\tau\rangle) \subseteq K$. Because $\mathcal{B} = (1, \alpha, \alpha^2, \zeta_3, \zeta_3\alpha, \zeta_3\alpha^2)$ is a $\mathbf{Q}$-basis for K, there exist unique $a_{i,j} \in \mathbf{Q}$ such that

$$\begin{aligned}
\beta &= \sum_{\substack{i\in\{0,1\},\\ j\in\{0,1,2\}}} a_{i,j}\zeta_3^i\alpha^j \\
&= a_{0,0}1 + a_{0,1}\alpha + a_{0,2}\alpha^2 + a_{1,0}\zeta_3 + a_{1,1}\zeta_3\alpha + a_{1,2}\zeta_3\alpha^2
\end{aligned} \tag{4}$$

Because $\sigma^2\tau \in \mathrm{Gal}(K : \mathbf{Q}) = \mathrm{Aut}(K : \mathbf{Q})$, it is a field homomorphism that fixes all elements of $\mathbf{Q}$. In particular, it fixes each $a_{i,j}$. Using these facts and our computation of $\sigma^2\tau$ on generators of $K : \mathbf{Q}$ in equation (2), we compute

$$\begin{aligned}
\sigma^2\tau(\beta) = \sigma^2\tau\left(\sum_{\substack{i\in\{0,1\},\\ j\in\{0,1,2\}}} a_{i,j}\zeta_3^i\alpha^j\right) &= \sum_{\substack{i\in\{0,1\},\\ j\in\{0,1,2\}}} a_{i,j} \cdot (\sigma^2\tau(\zeta_3))^i \cdot (\sigma^2\tau(\alpha))^j \\
&= a_{0,0} \cdot 1 + a_{0,1} \cdot \sigma^2\tau(\alpha) + a_{0,2} \cdot (\sigma^2\tau(\alpha))^2 \\
&\quad + a_{1,0} \cdot \sigma^2\tau(\zeta_3) + a_{1,1} \cdot \sigma^2\tau(\zeta_3) \cdot \sigma^2\tau(\alpha) + a_{1,2} \cdot \sigma^2\tau(\zeta_3) \cdot (\sigma^2\tau(\alpha))^2 \\
&= a_{0,0}1 + a_{0,1}\zeta_3^2\alpha + a_{0,2}\zeta_3\alpha^2 + a_{1,0}\zeta_3^2 + a_{1,1}\zeta_3\alpha + a_{1,2}\alpha^2 \\
&= a_{0,0}1 - a_{0,1}(1+\zeta_3)\alpha + a_{0,2}\zeta_3\alpha^2 - a_{1,0}(1+\zeta_3) + a_{1,1}\zeta_3\alpha + a_{1,2}\alpha^2 \\
&= (a_{0,0} - a_{1,0})1 - a_{0,1}\alpha + a_{1,2}\alpha^2 - a_{1,0}\zeta_3 + (a_{1,1} - a_{0,1})\zeta_3\alpha + a_{0,2}\zeta_3\alpha^2
\end{aligned} \tag{5}$$

By hypothesis, $\beta \in \mathcal{F}(\langle \sigma^2\tau \rangle)$, so

$$\sigma^2\tau(\beta) = \beta$$

That is, the right sides of equations (4) and (5) are equal. Because $\mathcal{B}$ is a $\mathbf{Q}$-basis (so, in particular, it is linear independent over $\mathbf{Q}$), for each basis element, the corresponding coefficients in these equations are equal. This gives a system of six linear equations in $\mathbf{Q}$:

$$\begin{aligned} 1 &: a_{0,0} = a_{0,0} - a_{1,0} & \zeta_3 &: a_{1,0} = -a_{1,0} \\ \alpha &: a_{0,1} = -a_{0,1} & \zeta_3\alpha &: a_{1,1} = a_{1,1} - a_{0,1} \\ \alpha^2 &: a_{0,2} = a_{1,2} & \zeta_3\alpha^2 &: a_{1,2} = a_{0,2} \end{aligned}$$

This system of equations implies

$$a_{0,1} = 0 \qquad a_{1,0} = 0 \qquad a_{1,2} = a_{0,2} \qquad a_{0,0}, a_{1,1} \in \mathbf{Q}$$

(The final expression simply states that $a_{0,0}$ and $a_{1,1}$ are free parameters.) That is, if $\beta \in \mathcal{F}(\langle \sigma^2\tau \rangle)$, then β has the form

$$\beta = a_{0,0}1 + a_{1,1}\zeta_3\alpha + a_{0,2}(\alpha^2 + \zeta_3\alpha^2)$$

for some $a_{0,0}, a_{1,1}, a_{0,2} \in \mathbf{Q}$.[1]

The first two terms are in $\mathbf{Q}(\zeta_3\alpha)$. What about the last term? Using the relation $\zeta_3^2 = -(1+\zeta_3)$, we compute

$$\alpha^2 + \zeta_3\alpha^2 = (1+\zeta_3)\alpha^2 = -\zeta_3^2\alpha^2 = -(\zeta_3\alpha)^2 \in \mathbf{Q}(\zeta_3\alpha)$$

[1] If you like to think in matrices, then we can reinterpret our work here in that language. Having chosen a basis $\mathcal{B}$ for the $\mathbf{Q}$-vector space K, we get a matrix $M_{\mathcal{B}}(\sigma^2\tau)$ for the linear transformation $\sigma^2\tau : K \to K$. For our basis $\mathcal{B} = (1, \alpha, \alpha^2, \zeta_3, \zeta_3\alpha, \zeta_3\alpha^2)$, we get

$$M_{\mathcal{B}}(\sigma^2\tau) = \begin{pmatrix} 1 & & & -1 & & \\ & -1 & & & & \\ & & & & & 1 \\ & & & -1 & & \\ & -1 & & & 1 & \\ & & 1 & & & \end{pmatrix}$$

Recall that the columns of this matrix are the coefficients of the linear combination with respect to the chosen basis $\mathcal{B}$ of each basis vector in $\mathcal{B}$; that is, $M_{\mathcal{B}}(\sigma^2\tau(\zeta_3^i\alpha^j))$. Given an arbitrary $\beta \in K$, its unique $\mathbf{Q}$-linear combination with respect to the basis $\mathcal{B}$ given in equation (4) writes as the 6×1 matrix (column vector)

$$M_{\mathcal{B}}(\beta) = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{1,0} & a_{1,1} & a_{1,2} \end{pmatrix}^t$$

Multiplying $M_{\mathcal{B}}(\sigma^2\tau)$ by $M_{\mathcal{B}}(\beta)$ gives a 6×1 matrix, equal to $M_{\mathcal{B}}(\sigma^2\tau(\beta))$, whose entries are the coefficients in equation (5). Setting this matrix equal to $M_{\mathcal{B}}(\beta)$ gives the six linear equations we listed above.

Note that, in this matrix view, solving

$$M_{\mathcal{B}}(\sigma^2\tau)M_{\mathcal{B}}(\beta) = M_{\mathcal{B}}(\beta)$$

is equivalent to solving

$$(I - M_{\mathcal{B}}(\sigma^2\tau))M_{\mathcal{B}}(\beta) = 0$$

where I denotes the 6×6 identity matrix. That is, to compute the fixed field of an element of the galois group, we can compute the eigenspace associated to the eigenvalue 1 for that element.

Remember, $\mathbf{Q}(\zeta_3\alpha)$ denotes the field generated by $\zeta_3\alpha$ over $\mathbf{Q}$. It contains $\mathbf{Q}$ and $\zeta_3\alpha$, and it is closed under the field operations. Thus, in particular, it also contains $(-1)(\zeta_3\alpha)^2$, as we asserted above. The same logic shows that $\beta \in \mathbf{Q}(\zeta_3\alpha)$. Because $\beta \in \mathcal{F}(\langle\sigma^2\tau\rangle)$ was arbitrary, we conclude that $\mathcal{F}(\langle\sigma^2\tau\rangle) \subseteq \mathbf{Q}(\zeta_3\alpha)$. Combining this with equation (3), we conclude that $\mathcal{F}(\langle\sigma^2\tau\rangle) = \mathbf{Q}(\zeta_3\alpha)$, as desired.